REMARKS

The Examiner has objected to the drawings. Substitute drawings are submitted herewith for approval by the Examiner.

The Examiner has further objected to the claims for informalities. In response, applicant has clarified the claims to avoid such objections.

Still yet, the Examiner has rejected Claims 4, 6, 13, 15, 20, 22 and 24 under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point and distinctly claim the subject matter which applicant regards as the invention. In response, applicant has clarified the claims to avoid such rejection.

The Examiner has rejected Claims 1, 2, 8-11, 17-20, 26, and 27 under 35 U.S.C. 102(b) as being anticipated by U.S. Patent No. 5,557,742 to Smaha et al. Applicant respectfully disagrees with such rejection.

In particular, the Examiner indicates that Smaha teaches receiv[ing] an audit trail, stor[ing] specified data in an even data structure (60), compare[ing] data against the contents of the information modules (62,64,66) using complete query (84) and compare[ing] one or more data to criteria for detecting an intrusion. More specifically, a misuse engine is employed that uses queries stored in a signature data structure (108) to determine intrusions.

Even if this statement were to be true, it appears that the Examiner has merely made an attempt to identify the following claim limitations in the prior art:

"running the auditing system to produce an audit log....
examining the audit log to detect patterns for intrusion detection purposes."

However, the Examiner's rationale fails to address applicant's claimed "configuring the auditing system to record the at least one target attribute in response to detecting the at least one

auditing criterion." The most relevant mention of any sort of criteria-based action in Smaha is in the following excerpt:

> "Computer program 26 selection of misuses that block 128 represents allows selecting misuses without requiring user input. For example, this includes programs that load previously selected misuses into misuse engine 30 or programs that dynamically select the misuses for which to search based on a set of criteria." (col. 9, lines 13-19, emphasis added).

Such criteria merely indicates the misuses for which the system is to "search." In sharp contrast, applicant teaches and claims "recording" specified attributes in response to triggering criteria.

Not only is applicant's claimed criteria-based recording of specified attributes not disclosed, taught or suggested by Smaha, but such feature would be unobvious, since Smaha does not even consider the problem which applicant's claimed invention solves. As indicated on page 11, first paragraph of the originally file specification: by selectively recording target attributes, the present invention can reduce the amount of data that is recorded during the auditing process. This makes it practical to record data that is read or written during system calls without overwhelming the storage capacity, processing power and/or data transfer bandwidth of a computer system.

In order to emphasize this advantage and further distinguish the criteria-based search for misuses of Smaha, applicant now claims "a size of the audit log [being] reduced when the auditing system is run prior to the examination for detection of the patterns." This claimed feature thus clearly distinguishes Smaha's criteria-based search for misuses, by indicating that applicant's criteria-based recording is done, at least in part, prior to applicant's claimed "examining" of the audit log to detect patterns for intrusion detection purposes. Only applicant teaches and claims criteria-based recording of specified attributes to overcome the foregoing problem.

The Examiner is reminded that a claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described in a single prior art reference. *Verdegaal Bros. v. Union Oil Co. Of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). Moreover, the identical invention must be shown in as complete detail as contained in

the claim. *Richardson v. Suzuki Motor Co.*868 F.2d 1226, 1236, 9USPQ2d 1913, 1920 (Fed. Cir. 1989). The elements must be arranged as required by the claim. This criteria has simply not been met by the Smaha reference, especially in view of the amendments made hereinabove.

The Examiner continues by rejecting Claims 4, 6, 13, 15, 22, and 24 under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,557,742 to Smaha et al. applied to Claim 1 above, and further in view of U.S. Patent No. 6,584,508 to Epstein et al.

Specifically, the Examiner relies on the following excerpt of Epstein to make a prior art showing of the claim limitations below:

"wherein the at least one target attribute includes:
an argument from a system call;
a parameter of a process making the system call;
data read during the system call;
data written during the system call;
a parameter of a file involved in the system call; and
a parameter relating to a network communication involved in the system call" (See Claim 4 et al.)

"wherein the at least one auditing criterion includes:
a user identifier for a process that is making a system call;
an identifier for an application program from which the system call is being made; and
an identifier for a file being accessed by the system call." (See Claim 6 et al.)

"As illustrated in FIG. 3, operating within the UNIX environment are programs 302A and 302B. Program 302B is an unwrapped program whose system calls pass directly to an internal application programming interface (API). Program 302A, on the other hand, is "wrapped" by wrapper 310. As illustrated, the kernel loadable module intercepts all system calls as they are made by a program 302A, and passes the system calls to wrapper 310 based on criteria (i.e., a wrapper specification (WS)) specified when wrapper 310 is loaded. In this framework, wrapper 310 runs in kernel mode and its execution environment is provided in the kernel loadable module. This execution environment is referred to as the wrapper enforcement layer (WEL).

> The WEL tracks running processes and evaluates activation criteria at appropriate times to activate new wrapper instances for processes. These wrapper instances wrap their processes by intercepting some or all of the system calls that are made by the process. This interception effectively puts the wrappers in complete control of their processes' interactions with the operating system and with other processes. For each system call, wrappers can observe and/or modify the parameters specified by the caller and the values returned by the operating system." (col. 5, lines 32-55)
>
> "As can be appreciated, some system calls are more likely to indicate an attempted subversion. For example, for most proxies an exec call, an attempt to bind ports other than that assigned to the proxy, or an attempt to read /etc/passwd is a sure sign of a break-in attempt, while attempts to read other files may more likely indicate an error in the wrapper. In one embodiment, interfacing with the intrusion detection system is performed by writing records to a log file, and having a user space daemon read the log file and forward the relevant records to the intrusion detection system for processing." (col. 6, lines 58-67)
>
> "The software wrappers provide for relatively small specifications of the allowed behavior of the associated multi-part proxy components. Security of the firewall components are thereby improved." (col. 3, lines 29-32)

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991). Applicant respectfully asserts that at least the first and third elements of the *prima facie* case of obviousness have not been met.

Most importantly, with respect to the third element of the *prima facie* case of obviousness, various claimed features are clearly missing from the Examiner's proposed combination. For example, such excerpts clearly fail to disclose, teach or suggest the combination of "an argument from a system cal; a parameter of a process making the system call; data read during the system call; data written during the system call; a parameter of a file involved in the system call; and a parameter relating to a network communication involved in the system call." (See Claim 4 et al.) Further lacking is applicant's claimed combination of "a user identifier for a process that is making a system

call; an identifier for an application program from which the system call is being made; and an identifier for a file being accessed by the system call." (See Claim 6 et al.)

Even still, the Examiner has rejected Claims 5, 14, and 23 under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,557,742 to Smaha et al. applied to Claim 1 above, and further in view of U.S. Patent No. 5,623,601 to Vu. In response, applicant contends that the present claims are allowable by virtue of being dependent on independent claims which are deemed allowable for the reasons set forth hereinabove.

Finally, Claims 3, 7, 12, 16, 21, and 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,557,742 to Smaha et al. Specifically, the Examiner has admitted that the subject matter of the instant claims are not disclosed, taught or suggested by Smaha, but then invokes Official Notice regarding such features.

In response, applicant formally requests a specific showing of the subject matter in ALL of the claims in any future action. Note excerpt from MPEP below.

> "If the applicant traverses such an [Official Notice] assertion the examiner should cite a reference in support of his or her position." See MPEP 2144.03.

A notice of allowance is respectfully requested. In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 505-5100. The Commissioner is authorized to charge any additional fees or credit any overpayment to Deposit Account No. 50-1351 (Order No. NAI1P250).

Respectfully submitted,

Kevin J. Zilka
Registration No. 41,429

P.O. Box 721120
San Jose, CA 95172-1120
408-505-5100